UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,505	12/03/2003	Robert Stoner	COS97083C1	3775

25537 7590 05/15/2009

VERIZON
PATENT MANAGEMENT GROUP
1320 North Court House Road
9th Floor
ARLINGTON, VA 22201-2909

EXAMINER	
TRAN, MYLINH T	

ART UNIT	PAPER NUMBER
2179	

NOTIFICATION DATE	DELIVERY MODE
05/15/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@verizon.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/725,505
Filing Date: December 03, 2003
Appellant(s): STONER ET AL.

Phouphanomketh Ditthavong
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 01/08/09 appealing from the Office action mailed 01/03/08.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5504921	Dev et al.	04/1996

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-38 are rejected under 35 U.S.C. 102(b) as being anticipated by Dev et al. [US.5,504,921].

As to claims 1 and 21, Dev et al. shows a communications network having first means for receiving communication of original messages generated from one or more network element subsystems (column 3, lines 38-55 and column 13, lines 1-15), the network element subsystems including console connections and application connections (column 5, lines 1-10, console connections and application connection would be one of the parts in the network);

means for mapping text of a received original message to one or more of a plurality of alarm attributes (column 4, lines 54-65 and column 12, lines 32-50) and means for determining the presence of an alarm condition from said one or more attributes (column 8, lines 27-55) and generating one or more responses according to said type of alarm condition (column 8, lines 41-55); means for enabling a remotely located user access to said one or more network elements via a display interface at a remote terminal (column 3, lines 28-55) and a said response including automatically presenting said remotely located user of an alarm condition at a network element via said display interface, said remotely located user being enabled to access said network element from said remote terminal for further responsive action thereof (column 14, lines 41-60).

As to claims 2 and 20, Dev et al. discloses said first server means includes a terminal server means physically connected to a console port I/O of each said network element, said remotely located user having access to said console port via said user interface (column 4, line 65 through column 5, line 1-17).

As to claims 3 and 23, Dev et al. shows the first server means includes means for receiving communication of original textual messages from a network application running on said network element, said first server means including a mailbox facility means for receiving said alarm messages (column 3, lines 35-60).

As to claim 4, Dev et al. teaches the network application running on said network element is a Log Management Facility application (column 3, lines 1-60).

As to claims 5 and 24, Dev et al. discloses means for presenting an indication of said alarm condition to said remotely located user via a network connection (column 2, lines 50-64).

As to claims 6 and 25, Dev et al. shows "graphical icon being color-coded to indicate alarm condition severity" (column 12, lines 16-67).

As to claim 7, Dev et al. demonstrates the terminal server means including a telnet terminal server (column 5, lines 1-10).

As to claim 8, Dev et al. teaches means for enabling a remotely located user access to said one or more network elements includes a network connection (column 2, lines 35-67).

As to claims 9 and 27, Dev et al. shows network socket connection is pursuant to a TCP/IP protocol (column 3, lines 28-62).

As to claim 10, Dev et al. discloses means for mapping text of a received original message to one or more of a plurality of alarm attributes includes utilizing regular expression matching (column 9, lines 40-65).

As to claims 11 and 29, Dev et al. teaches the message attributes include one or more selected from the group comprising: originating network element, time, alarm severity level, alarm mnemonic, alarm description, process name, and network element name (column 8, lines 1-13).

As to claims 12 and 30, Dev et al. discloses means for determining presence of an alarm condition from said one or more attributes includes means for applying configuration rules to said alarm attributes, said configuration rules stored as text in a first storage means at or near said first means and accessible therefrom (column 9, lines 40-65 and column 12, lines 15-51).

As to claims 13 and 31, Dev et al. teaches text editor means for enabling a user to modify existing configuration rules stored in said storage means via said user display interface, said text editor means further enabling said user to generate new configuration rules for storage in said storage means, said new configuration rules creating a new alarm condition (column 9, lines 5-67).

As to claims 14,15,32 and 33, Dev et al. shows configuration rules further provides a sifting operation for sifting through said attributes to match said alarm condition with a pre-determined alarm condition and the sifting means operation enables an alarm message to be terminated if a match with a pre-determined alarm condition is found (column 14, lines 41-60).

As to claims 16,17,34 and 35, Dev et al. teaches configuration rules further provide a logging operation for automatically logging alarm conditions in a second storage means at or near said first means and accessible therefrom and means for generating reports including past alarm conditions stored in said second storage means (column 9, lines 43-67).

As to claims 18 and 19, Dev et al. discloses a response action includes initiating transmission of an e-mail message and a response action includes

initiating transmission of a paging message and command procedure (column 11, lines 40-55).

As to claim 22, Dev et al. shows providing a physical connection between each said network element and a terminal server device enabling remote access to said one or more network elements via said user display interface (column 3, line 35-through column 4, line 15).

As to claim 26, Dev et al. show providing a network socket connection to enable said remotely located user access to said one or more network elements (column 3, lines 62).

As to claim 28, Dev et al show the step of mapping text including utilizing regular expression matching (column 8, lines 30-55).

As to claim 36, Dev et al. teaches a transaction server and a communications server; the transaction server and communications server and to transmit the same over a network link (column 5, lines 1-17); a telecommunications network alarm monitoring server linked to the terminal server of the service control point over the network link; a network alarm monitoring process to map the event messages to an alarm data structure and a network link to the telecommunications network alarm monitoring server to enable transmission of messages by the network alarm monitoring server in response to recognized alarm condition (column 3, lines 38-55 and column 13, lines 1-15)

As to claim 37, Dev et al. teaches access is enabled to the terminal server is over an Internet Protocol network (column 4, lines 1-15).

As to claim 38, the claim is analyzed as previously discussed with respect to claims 36 and 37.

(10) Response to Argument

Appellant has argued that Dev does not teach or suggest the claimed feature of "the network element subsystems including console connections and application connections that it is the network element subsystems that generate the original textual message".

However, as defined in the specification, a Alarm Monitoring Systems server receives a continuous stream of messages generated by two sources: 1) console connection and 2) application connections. Application connection is using either TCP/IP or DECNet.TM. TCP/IP is defined in the Microsoft Press Computer Dictionary as "Transport Control Protocol/Interface Program". Data delivered via console connections using telnet protocols. According to Collegiate Dictionary, a telnet is defined as "a telecommunications protocol providing specifications for emulating a remote computer terminal so that one can access a distant computer and function online using an interface that appears to be part of the user's local system".

Based on the above definitions of Telnet and TCP/IP, console connection and application connection are taught in the Dev's system.

Communications could not be established between network elements if there were no connections and processing couldn't be performed without application

connections. Dev also cited "the virtual network further includes model relations representing relations between the network entities. The system also includes means for transferring network data from the network entities to the corresponding models in the virtual network....The model relations define both network connections between network devices and hierarchical relationships between network entities." (column 2, lines 28-45).

Dev also teach the network element subsystems that generate the original textual message at column 4, lines 59-65 by cited "In some cases, the network devices send status information to the network management system automatically without polling. In either case, the information received from the network is processed so that the operation status, faults and other information pertaining to the network are presented to the user in a systematized and organized manner." It is clear that the network devices send status information to the network management system. Dev also teaches generating textual message by cited "the event message provides specific information about events, including alarms that have occurred in a given model. The events pass from the model to an event log manger which records the event in the external database...."(column 7, lines 35-42); and "when an alarm event occurs in a model, a notice of the alarm event is sent to an alarm log and to the event log. The alarm log selects the most severe alarm for each model which is registering an alarm. The alarms are sent to an alarm window in the user interface...Alarm log messages include the following parameters: alarm condition, alarm cause,

alarm status, alarm security data, alarm clear switch and alarm unique ID" (column 8, lines 1-10).

Appellant also argued that Dev et al. do not teach or suggest "means for mapping text of received original message to one or more of a plurality of alarm attributes." However, Dev teaches sending status information to a network management system and presenting "operational status, faults and other information pertaining to the network" (column 4, lines 54-65 and column 12, lines 32-50).

Appellant's attention is directed to column 8, lines 22-53, "In operation, at a specified time model 144 initiates polling of network device 44 in step 200 in order to obtain an update of the status of network device 44. The model 144 sends a request to the device communication manager 14 to poll network device 44. The device communication manager 14 converts the request to the required protocol for communication with network device 44 and sends the message. The requested information may, for example, be the number of packets sent on the network in a given time and the number of errors that occurred. When the requested information is returned to model 144, the corresponding attributes in model 144 are updated in step 206 and an error rate inference handler is triggered. The error rate inference handler in step 208 calculates the error rate for network device 44. If the error rate is within prescribed limits (step 210), an error rate attribute is updated, and the new information is logged into the database (step 212). If the calculated error

rate is above a predetermined limit, an error alarm inference handler is triggered. The error alarm inference handler may shut off the corresponding network device 44 and send an alarm to the user interface in step 214. The alarm is also logged in the database. If the network device 44 is shut off in response to a high error rate, a condition attribute in model 144 is updated to reflect the off condition in step 216. If no response was received from the network device 44 when it was polled (step 218), a fault isolation inference handler is triggered in step 220. The fault isolation inference handler operates as described below to determine the network component which caused network device 44 to fail to respond to the poll. When the cause of the fault is determined, a fault message is sent to the user interface."

In Dev, the message is determined its type and send an alarm based on the type of the message. Therefore, the mapping text is taught by mapping the text attribute to condition attribute model. Dev teaches a telecommunications network alarm monitoring server linked to the terminal server of the service control point over the network link; a network alarm monitoring process to map the event messages to an alarm data structure and a network link to the telecommunications network alarm monitoring server to enable transmission of messages by the network alarm monitoring server in response to recognized alarm condition (column 3, lines 38-55 and column 13, lines 1-15).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Mylinh Tran/

AU 2179

Conferees:

/Weilun Lo/

Supervisory Patent Examiner, Art Unit 2179

/Ba Huynh/

Primary Examiner, Art Unit 2179